DETAILED ACTION

1. The response of 4/30/2008 was received and considered.

2. Claims 1-24 are pending.

Information Disclosure Statement

3. The information disclosure statement filed 4/30/2008 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered. Only U.S. Patents, U.S. Patent Application Publications and U.S. Pending Applications submitted are considered.

4. It is further noted that applicant has submitted via the information disclosure statements of 4/30/2008, an extensive list of 118 references. In light of this extensive submission, the Examiner will assume that the disclosures are cumulative. If Applicant is aware of anything in the references that is material to patentability, Applicant is requested to clearly identify it to the Examiner in response to this action.

Specification

5. The disclosure is objected to because of the following informalities: PP. 1-2 of the specification list similar patent applications using Attorney docket numbers. Applicant is reminded that the docket numbers should be replaced with application or patent numbers (and any other information updated), as necessary.

Appropriate correction is required.

Response to Arguments

6. Applicant's arguments filed 4/30/2008 have been fully considered but they are not persuasive.

7. Applicant's response refers to the arguments previously filed in the appeal and reply briefs, filed on 8/29/2007 and 1/22/2008, respectively. Since Applicant's arguments in the appeal brief have previously been considered and responded to, Applicant is referred to the previous Examiner's Answer. The arguments in the reply brief will be discussed below.

a. The reply brief (p. 4) argues that the examiner's interpretation that the claimed "second key" is equivalent to Richard's PK and SK. However, as previously submitted, the Examiner's position is that the scope of Applicant's claim language encompasses such a feature.

b. The reply brief (p. 5) argues that PK and SK are not encrypted by CCK_1. However, as previously submitted, CCK_1 encrypts PK and PK encrypts SK and the Examiner's position is that the scope of Applicant's claim language encompasses this scenario ("encrypting the second key with the registration key", i.e. CCK_1 is used to encrypt SK).

c. The reply brief (p. 5) argues that the Examiner's previous argument that "the mathematical process takes multiple steps" is unfounded (i.e. the Examiner submitted that CCK_1 encrypts SK by CCK_1 encrypting PK where PK encrypts SK under the

reasoning that without CCK_1 decrypting PK, SK could not be recovered). The previous position is maintained.

d. The reply brief (p. 6) argues that Applicant's arguments are not contradictory (i.e. the Examiner previously argued a contradiction because Applicant argued that the claimed second key cannot be equated to SK and PK because SK and PK are different values. The Examiner noted that Applicant claims a key updated in two parts. Therefore, it is maintained that because Applicants claims require the second key to be two different values, this interpretation is reasonable.

e. The reply brief (pp. 6-7) appears to argue that the Examiner's interpretation of "encrypting" is not supported by the standard meaning. However, as explained above, Richards discloses CCK_1 encrypting PK, PK encrypting SK and SK encrypting the content. As such, the Examiner believes that it is a reasonable interpretation to read that Richards discloses encrypting a second key (PK and SK) with a first key (CCK, because Richards discloses [PK]CCK_1,[SK]PK).

f. The reply brief (p. 8) argues the remaining rejections using the above rationale. Therefore, the Examiner refers to the above responses to Applicant's arguments.

8. Lastly, the Examiner notes that there is a disagreement of interpretation between what can or cannot be interpreted as "encrypting" (i.e. using a key encrypting a first value that is used to encrypt a second value versus mathematically combining the key and the second value) and what can or cannot be interpreted as a "key" (i.e. SK and PK being two separate values). In the interest of advancing prosecution of the instant application, it is noted that an amendment to the

independent claims could render the Examiner's argument moot. For example in claim 1, "wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel, where the two parts are combined to form the second key". Since this limitation (that the second key, which is updated in two parts is ultimately a single value) is considered by Applicant as the proper interpretation of the claim language (see appeal and reply briefs), such a limitation or similar will be commensurate with the intended scope of Applicant's claims.

Claim Rejections - 35 USC § 101

9. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

10. Claims 22-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

g. The "means" recited in claims 22-23, in accordance with the specification, can be software, per se, which does not fall within one of the statutory classes of invention (i.e. the software is not tangibly embodied on a storage medium).

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for

> patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

12. Claims 1-5, 10-11, 13-16 & 18-24 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,690,795 to **Richards**.

Regarding claims 1-5, 11, 13-14 & 22-24, Richards discloses determining a registration key (UEV) specific to a participant (set top box) in a transmission (Fig. 26, #130 & col. 20, lines 61-67), determining a first key (CCK_1, Fig. 26, #133), encrypting the first key (CCK_1) with the registration key (Fig. 26, #133), sending the encrypted first key ([CCK_1]UEV) to the participant in the transmission (set top box, Fig. 26, #133), determining a second key (PK and SK) for decrypting content on a broadcast channel (Fig. 26, #159), encrypting the second key with the first key ([PK]CCK_1, [SK]PK) updating the first key (CCK) after a first time period has elapsed (Fig. 23) and updating the second key (SK and PK) after a second time period has elapsed, wherein the second key is updated in two parts (SK and PK), the first part (PK) known to the participant in the transmission (PK must be known to decrypt SK, Fig. 26 & col. 13, lines 47-49) and a second part (SK) send on the broadcast channel (Fig. 26).

Regarding claim 10, Richards discloses transmitting the encrypted first key (PK) and transmitting the encrypted second key (SK, col. 9, line 58 – col. 10, line 5).

Regarding claims 15 & 16, Richards discloses in a wireless system (col. 20, lines 61-67) determining a registration key (UEV) specific to a participant (set top box) in a transmission (Fig. 26, #130), determining a first key (CCK_1, Fig. 26, #133), encrypting the first key (CCK_1) with the registration key (Fig. 26, #133), sending the encrypted first key ([CCK_1]UEV) to the participant in the transmission (set top box, Fig. 26, #133), determining a

second key (PK and SK), encrypting the second key with the first key ([PK]CCK_1, [SK]PK) updating the first key (CCK) after a first time period has elapsed (Fig. 23) and updating the second key (SK and PK) after a second time period has elapsed, wherein the second key is updated in two parts (SK and PK), the first part (PK) known to the participant in the transaction and a second part (SK) sent on a broadcast channel (Fig. 26), a user identification unit (set-top box, col. 4, lines 55-62), operative to recover a short-time key (SK) for decrypting a broadcast message (content, col. 9, lines 11-33), comprising a processing unit (decryption hardware) to decrypt key information (col. 9, lines 11-33) and a mobile equipment unit (decryption hardware) adapted to apply the short-time key for decrypting the broadcast message (content, col. 4, lines 55-62 & col. 9, lines 11-33).

Regarding claim 18, Richards discloses the memory storage unit storing a broadcast access key (PK) and wherein the processing unit decrypts the short-time key (SK) using the broadcast access key (PK, col. 5, lines 45-64 & col. 9, lines 56-63).

Regarding claim 19, Richards discloses the short-time key (SK) being updated at a first frequency (col. 9, lines 32-36 & Fig. 16).

Regarding claim 20, Richards discloses the broadcast access key (PK) being updated at a second frequency less than the first frequency (Figs. 9 & 10).

Regarding claim 21, Richards discloses a video service (col. 2, lines 39-55).

13. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Richards**, as applied to claim 4 above, in further view of "FOLDOC, Free On-Line Dictionary Of Computing" by **LinuxGuruz**. Richards discloses using the system for distributing information on computer

networks, but lacks specifically Internet Protocol packets. However, LinuxGuruz teaches that Internet Protocol packets are widely used on Ethernet networks for packet routing (§Internet Protocol). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to broadcast Internet Protocol packets. One of ordinary skill in the art would have been motivated to perform such a modification because Internet Protocol packets are used on Ethernet networks, as taught by LinuxGuruz (§Internet Protocol).

14. Claims 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Richards**, as applied to claim 3 above, in further view of Applied Cryptography, Second Edition by **Schneier**.

Regarding claim 7, Richards lacks calculating a registration key information message and transmitting the registration key information message. However, Schneier teaches that no encryption key should be used for an indefinite period (p. 183, §8.10) and should be replaced (p. 184, ¶3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to update the registration key and hence calculate a registration key information message and transmit the registration key information message. One of ordinary skill in the art would have been motivated to perform such a modification to update the registration key, as taught by Schneier (pp. 183-184).

Regarding claim 8, Richards discloses calculating a first key (PK) information message (new encrypted key) and transmitting the first key information message (col. 10, lines 1-5).

Regarding claim 9, Richards discloses calculating a second key (PK) information message (new encrypted key) and transmitting the second key information message (col. 9, lines 58-62).

15. Claims 12 & 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Richards**, as applied to claims 11 & 15 above, in further view of U.S. Patent 6,073,122 to **Wool**. Richards discloses storing the second key (SK) in a memory storage unit (col. 5, lines 60-63), but lacks the first key stored in secure memory storage unit. However, Wool teaches that set-top boxes often contain secure memory to minimize piracy of encryption keys stored (col. 1, lines 44-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store the first key in a secure memory storage unit. One of ordinary skill in the art would have been motivated to perform such a modification to minimize piracy of encryption keys stored, as taught by Wool (col. 1, lines 44-52).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J. SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

June 3, 2008
/Michael J Simitoski/
Primary Examiner, Art Unit 2134